

CCSK Dumps

Certificate of Cloud Security Knowledge

<https://www.certleader.com/CCSK-dumps.html>



NEW QUESTION 1

What factors should you understand about the data specifically due to legal, regulatory, and jurisdictional factors?

- A. The physical location of the data and how it is accessed
- B. The fragmentation and encryption algorithms employed
- C. The language of the data and how it affects the user
- D. The implications of storing complex information on simple storage systems
- E. The actual size of the data and the storage format

Answer: D

NEW QUESTION 2

Your SLA with your cloud provider ensures continuity for all services.

- A. False
- B. True

Answer: A

NEW QUESTION 3

A security failure at the root network of a cloud provider will not compromise the security of all customers because of multitenancy configuration.

- A. False
- B. True

Answer: A

NEW QUESTION 4

Use elastic servers when possible and move workloads to new instances.

- A. False
- B. True

Answer: B

NEW QUESTION 5

Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?

- A. Infrastructure
- B. Datastructure
- C. Infostructure
- D. Applistructure
- E. Metastructure

Answer: A

NEW QUESTION 6

What are the primary security responsibilities of the cloud provider in the management infrastructure?

- A. Building and properly configuring a secure network infrastructure
- B. Configuring second factor authentication across the network
- C. Properly configuring the deployment of the virtual network, especially the firewalls
- D. Properly configuring the deployment of the virtual network, except the firewalls
- E. Providing as many API endpoints as possible for custom access and configurations

Answer: D

NEW QUESTION 7

CCM: In the CCM tool, is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

- A. Risk Impact
- B. Domain
- C. Control Specification

Answer: C

NEW QUESTION 8

What can be implemented to help with account granularity and limit blast radius with IaaS and PaaS?

- A. Configuring secondary authentication
- B. Establishing multiple accounts
- C. Maintaining tight control of the primary account holder credentials
- D. Implementing least privilege accounts

E. Configuring role-based authentication

Answer: B

NEW QUESTION 9

Which concept is a mapping of an identity, including roles, personas, and attributes, to an authorization?

- A. Access control
- B. Federated Identity Management
- C. Authoritative source
- D. Entitlement
- E. Authentication

Answer: D

NEW QUESTION 10

CCM: A company wants to use the IaaS offering of some CSP. Which of the following options for using CCM is NOT suitable for the company as a cloud customer?

- A. Submit the CCM on behalf of the CSP to CSA Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry that documents the security controls provided by CSPs
- B. Use CCM to build a detailed list of requirements and controls that they want their CSP to implement
- C. Use CCM to help assess the risk associated with the CSP
- D. None of the above

Answer: D

NEW QUESTION 10

Which cloud security model type provides generalized templates for helping implement cloud security?

- A. Conceptual models or frameworks
- B. Design patterns
- C. Controls models or frameworks
- D. Reference architectures
- E. Cloud Controls Matrix (CCM)

Answer: D

NEW QUESTION 15

Which statement best describes why it is important to know how data is being accessed?

- A. The devices used to access data have different storage formats.
- B. The devices used to access data use a variety of operating systems and may have different programs installed on them.
- C. The device may affect data dispersion.
- D. The devices used to access data use a variety of applications or clients and may have different security characteristics.
- E. The devices used to access data may have different ownership characteristics.

Answer: D

NEW QUESTION 20

Which of the following statements best defines the "authorization" as a component of identity, entitlement, and access management?

- A. The process of specifying and maintaining access policies
- B. Checking data storage to make sure it meets compliance requirements
- C. Giving a third party vendor permission to work on your cloud solution
- D. Establishing/asserting the identity to the application
- E. Enforcing the rules by which access is granted to the resources

Answer: D

NEW QUESTION 21

Which statement best describes the impact of Cloud Computing on business continuity management?

- A. A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.
- B. The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomes necessary.
- C. Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
- D. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
- E. Geographic redundancy ensures that Cloud Providers provide highly available services.

Answer: E

NEW QUESTION 23

How does virtualized storage help avoid data loss if a drive fails?

- A. Multiple copies in different locations

- B. Drives are backed up, swapped, and archived constantly
- C. Full back ups weekly
- D. Data loss is unavoidable with drive failures
- E. Incremental backups daily

Answer: A

NEW QUESTION 27

Your cloud and on-premises infrastructures should always use the same network address ranges.

- A. False
- B. True

Answer: A

NEW QUESTION 31

What should every cloud customer set up with its cloud service provider (CSP) that can be utilized in the event of an incident?

- A. A data destruction plan
- B. A communication plan
- C. A back-up website
- D. A spill remediation kit
- E. A rainy day fund

Answer: B

NEW QUESTION 34

Audits should be robustly designed to reflect best practice, appropriate resources, and tested protocols and standards. They should also use what type of auditors?

- A. Auditors working in the interest of the cloud customer
- B. Independent auditors
- C. Certified by CSA
- D. Auditors working in the interest of the cloud provider
- E. None of the above

Answer: B

NEW QUESTION 35

Which of the following statements best describes an identity federation?

- A. A library of data definitions
- B. A group of entities which have decided to exist together in a single cloud
- C. Identities which share similar attributes
- D. Several countries which have agreed to define their identities with similar attributes
- E. The connection of one identity repository to another

Answer: E

NEW QUESTION 37

ENISA: "VM hopping" is:

- A. Improper management of VM instances, causing customer VMs to be commingled with other customer systems.
- B. Looping within virtualized routing systems.
- C. Lack of vulnerability management standards.
- D. Using a compromised VM to exploit a hypervisor, used to take control of other VMs.
- E. Instability in VM patch management causing VM routing errors.

Answer: D

NEW QUESTION 38

A defining set of rules composed of claims and attributes of the entities in a transaction, which is used to determine their level of access to cloud-based resources is called what?

- A. An entitlement matrix
- B. A support table
- C. An entry log
- D. A validation process
- E. An access log

Answer: D

NEW QUESTION 40

What is true of a workload?

- A. It is a unit of processing that consumes memory
- B. It does not require a hardware stack
- C. It is always a virtual machine
- D. It is configured for specific, established tasks
- E. It must be containerized

Answer: A

NEW QUESTION 45

If there are gaps in network logging data, what can you do?

- A. Nothin
- B. There are simply limitations around the data that can be logged in the cloud.
- C. Ask the cloud provider to open more ports.
- D. You can instrument the technology stack with your own logging.
- E. Ask the cloud provider to close more ports.
- F. Nothin
- G. The cloud provider must make the information available.

Answer: C

NEW QUESTION 48

Which of the following is NOT a cloud computing characteristic that impacts incidence response?

- A. The on demand self-service nature of cloud computing environments.
- B. Privacy concerns for co-tenants regarding the collection and analysis of telemetry and artifacts associated with an incident.
- C. The possibility of data crossing geographic or jurisdictional boundaries.
- D. Object-based storage in a private cloud.
- E. The resource pooling practiced by cloud services, in addition to the rapid elasticity offered by cloud infrastructures.

Answer: B

NEW QUESTION 53

How can key management be leveraged to prevent cloud providers from inappropriately accessing customer data?

- A. Use strong multi-factor authentication
- B. Secure backup processes for key management systems
- C. Segregate keys from the provider hosting data
- D. Stipulate encryption in contract language
- E. Select cloud providers within the same country as customer

Answer: C

NEW QUESTION 58

Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

- A. False
- B. True

Answer: B

NEW QUESTION 63

CCM: A hypothetical start-up company called "ABC" provides a cloud based IT management solution. They are growing rapidly and therefore need to put controls in place in order to manage any changes in their production environment. Which of the following Change Control & Configuration Management production environment specific control should they implement in this scenario?

- A. Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant)-impacting (physical and virtual) applications and systemsystem interface (API) designs and configurations, infrastructure network and systems components.
- B. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned ormanaged user end-point devices (e.
- C. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
- D. All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.
- E. None of the above

Answer: A

NEW QUESTION 64

In the Software-as-a-service relationship, who is responsible for the majority of the security?

- A. Application Consumer
- B. Database Manager
- C. Application Developer
- D. Cloud Provider
- E. Web Application CISO

Answer: D

NEW QUESTION 66

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CCSK Exam with Our Prep Materials Via below:

<https://www.certleader.com/CCSK-dumps.html>